FastNetMon

Jon Nield
NetMcr #2, 20160811

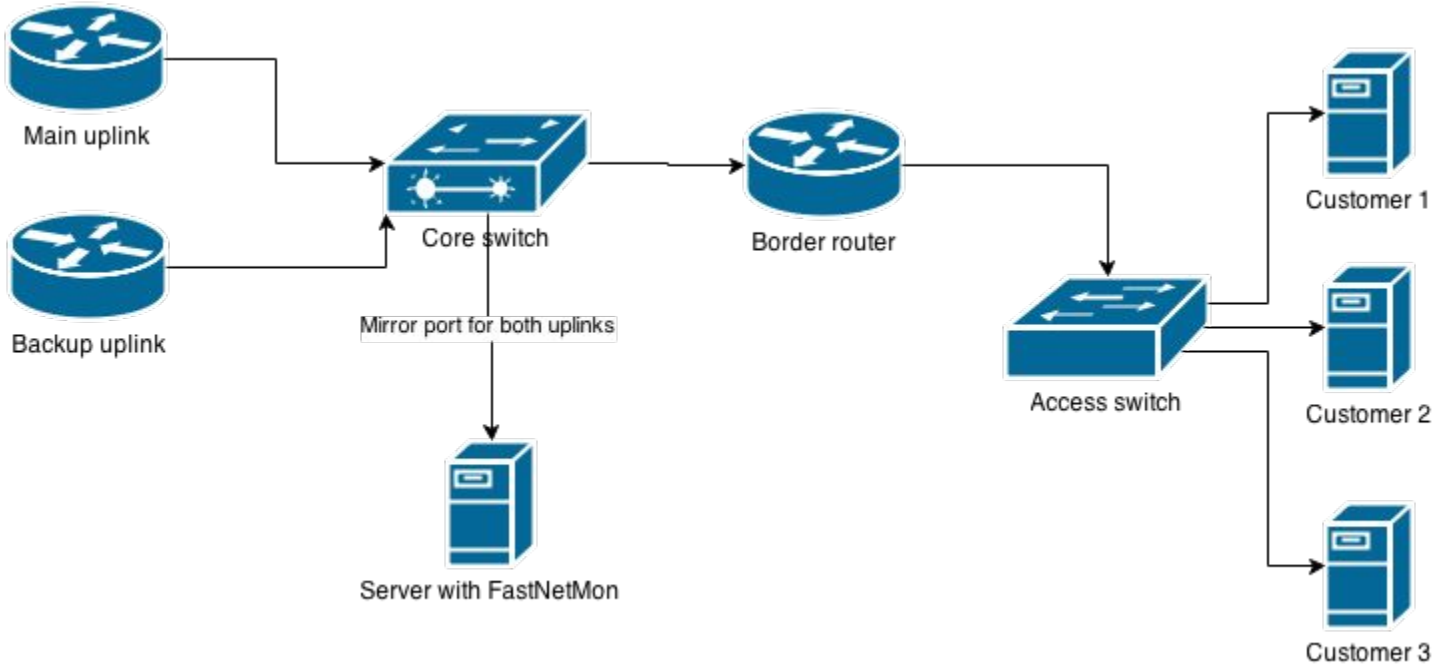
What is it?

- Open source real time black hole system
- Developed by Pavel Odintsov
- Available from https://github.com/pavel-odintsov/fastnetmon
- #fastnetmon on irc.freenode.net

Features

- Cross platform (Linux/BSD/OS X)
- Low resource requirements (70MiB, 20% CPU)
- Fast response times
- Customisable configuration
- Flexible response methods
- Works with ExaBGP/GoBGP

How does it work?



Sources of Network Data

- SFlow
- Netflow v5, v9, IPFIX
- Mirror port with support for PF_RING

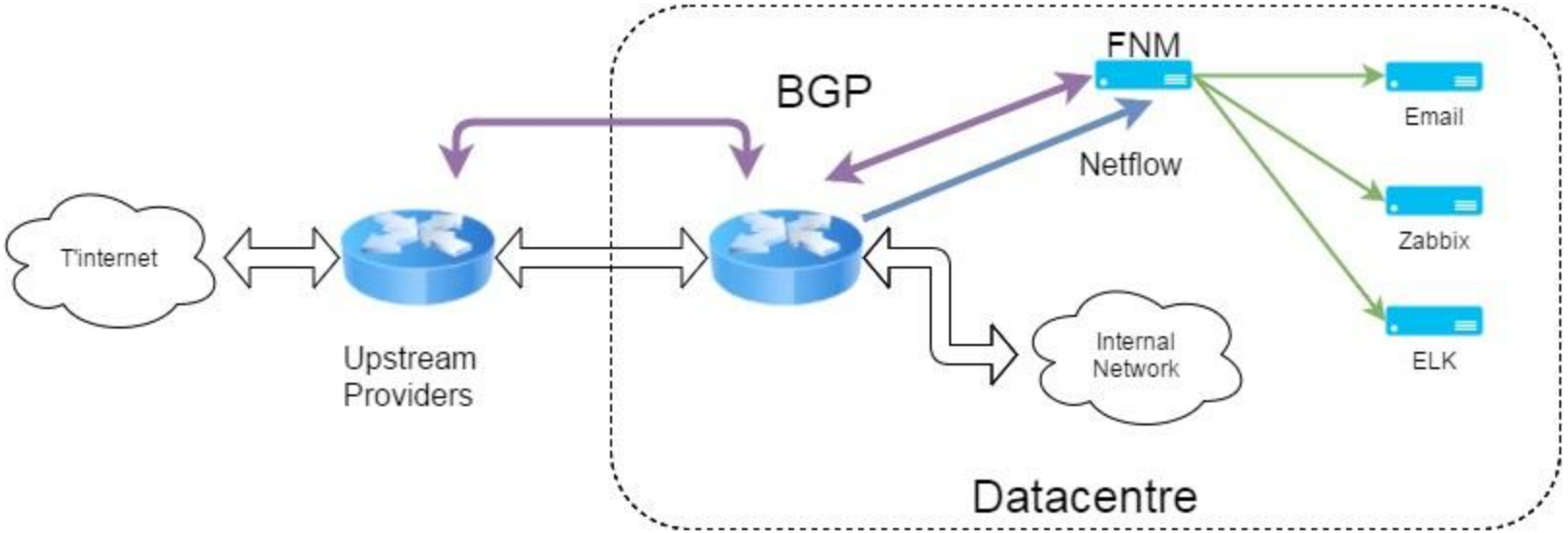
What it Looks Like in Use

```
FastNetMon 1.1.3 master git-030da794eefc5ae5c2fef61a5c79592981e07dcf FastVPS
Global bans enabled: True
Warns enabled: True
IPs ordered by: packets
Incoming traffic  411737 pps    953 mbps   2000 flows
1.2.3.4            15307 pps     23 mbps      0 flows
1.2.3.4             8900 pps     13 mbps      0 flows
1.2.3.4             6873 pps      2 mbps      0 flows
1.2.3.4             6571 pps      3 mbps      0 flows
1.2.3.4             5841 pps     12 mbps      0 flows
1.2.3.4             5796 pps      6 mbps      3 flows
1.2.3.4             4391 pps     17 mbps      0 flows
1.2.3.4             4032 pps     23 mbps      0 flows
1.2.3.4             4028 pps      1 mbps      0 flows
1.2.3.4             3671 pps     31 mbps      0 flows

Outgoing traffic             0 pps      0 mbps      0 flows
Internal traffic         32050 pps    117 mbps

Subnet load:
1.2.3.0/24         pps in: 127200   out: 0        mbps in: 217   out: 0
1.2.3.0/24         pps in: 70200    out: 0        mbps in: 81    out: 0
1.2.3.0/24         pps in: 61200    out: 0        mbps in: 79    out: 0
1.2.3.0/24         pps in: 55800    out: 0        mbps in: 96    out: 0
1.2.3.0/24         pps in: 55400    out: 0        mbps in: 100   out: 0
```

How We Use It


FNM
BGP
Email
Netflow
Zabbix
T'internet
ELK
Internal
Network
Upstream
Providers
Datacentre

Quirks in Practise

- Limited documentation
- Maintain two list of subnets
- Flow averages not accurate in the client
- Our modifications
  - https://github.com/ukfast/fastnetmon
  - Adds warning thresholds
  - Improved subnet matching (closer to most specific prefix)
  - Blanks at EOL in configuration files

Questions?